CHARTER MARK

PATENTS • DESIGNS
The Patent Office
COPYRIGHT • TRADE MARKS

INVESTOR IN PEOPLE

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

CERTIFIED COPY OF PRIORITY DOCUMENT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed

Dated 18 JAN 2002

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

The Patent Office

Cardiff Road
Newport
Gwent NP9 1RH

Request for a grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

1.	**Your reference**	P008760GB RWP
2.	**Patent application number** *(The Patent Office will fill in this part)*	**0008439.2**
3.	**Full name, address and postcode of the or of each applicant** *(underline all surnames)*	SONY UNITED KINGDOM LIMITED THE HEIGHTS BROOKLANDS WEYBRIDGE SURREY KT13 0XW UNITED KINGDOM
	Patents ADP number *(if you know it)*	6522700003
	If the applicant is a corporate body, give the country/state of its incorporation	UNITED KINGDOM
4.	**Title of the invention**	MATERIAL PROCESSING
5.	**Name of your agent** *(if you have one)*	D YOUNG & CO
	"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*	21 NEW FETTER LANE LONDON EC4A 1DA
	Patents ADP number *(if you have one)*	59006

6.	**If you are declaring priority from one or more earlier patent applications, give the country and date of filing of the or each of these earlier applications and (if you know it) the or each application number**	**Country**	**Priority application number** *(if you know it)*	**Date of filing** *(day/month/year)*

7.	**If this application is divided or otherwise derived from an earlier UK application, give the number and filing date of the earlier application**	**Number of earlier application**	**Date of filing** *(day/month/year)*

Material Processing

The present invention relates to a video and/or audio processing system and method.

It is known to use watermarks in video material to indicate the provenance of the material. However some video processing may damage or destroy a watermark.

According to the present invention, there is provided a video processing system for processing video material including a reversible watermark, the system comprising a remover for removing the watermark, a processor for processing the video material from which the watermark has been removed, and an inserter for inserting a watermark into the processed material.

Thus the watermark is removed before processing and a watermark is inserted after processing, avoiding damage to a watermark. The watermark inserted after processing may be the same as the removed mark or may be different.

In principle such a system could be under the control of a user of the processor. However, if the user can control the removal and insertion process, he could indulge in fraud. Thus to prevent fraud the removal and insertion process is preferably automatic and independent of the user. Most preferably it is performed without the knowledge of the user. Thus the video processing system is closed with respect to the removal and insertion of watermarks.

The removal and insertion of watermark may involve the use of data enabling those processes. Preferably, the enabling data is an encryption key. The enabling data may be securely stored or generated in the processor. Alternatively, the enabling data may be stored in and retrieved from a separate, preferably secure, database. The database may be linked, e.g. via a suitable communications link, to the system. Preferably, the link provides secure transfer of the enabling data.

For a better understanding of the present invention, there will now be described, by way of example, an illustrative embodiment of the invention with reference to the accompanying drawings, in which:

Figure 1 is a schematic block diagram of an illustrative watermark insertion and removal system;

Figures 2 and 3 are schematic diagrams of data structures of UMIDs

Figure 4 is a schematic block diagram an illustrative data structure of a metadata base; and

Figures 5 and 6 are schematic diagrams of watermarking techniques.

Overview-Figure 1

Referring to Figure 1, a video processor processes video material input at input 632 and outputs processed video at output 630. The processor may be an editor, a special effects machine, a mixer or any other video processor. Whilst only one input and one output is shown, the processor may have a plurality of inputs and at least one output. If the processor is a mixer for example it has two or more inputs.

The processor has a user interface 644 having user controls (not shown) for controlling the processor.

The input material contains watermarks. Watermarks are described in the section *watermarks* below. Watermarks may be used to check the provenance of video material. Watermarks may identify the owners of the material. In a preferred embodiment of the invention , the watermarks identify the material (which we believe to be a novel idea). Most preferably the watermarks are based on UMIDs (which we believe to be a novel idea). UMIDs are described in the section *UMIDs* below.

In accordance with a preferred embodiment of the present invention, the processor is a closed system with respect to processing watermarks. That is the user has control only of the video processing but no control of, nor access to, the watermark processing. The watermark processing is automatic and invisible to the user.

Thus in accordance with the present embodiment, watermarks are automatically removed in a remover 640 before video processing in a processing stage

646, and watermarks are automatically inserted into the processed video after processing by an inserter 642. Removal and insertion of watermarks may require enablement by enabling data. That data may be stored and/or generated in the processor 644 or retrieved from a database 636 via a secure datalink 634. The enabling data preferably includes UMIDs for the watermarks inserted after processing.

In a preferred embodiment, the enabling data includes encryption keys for removing and inserting encrypted watermarks.

The database may store data for verifying the provenance of input material by checking the watermark against verification data which may be a UMID. The processor 648 may be disabled in the presence of material which fails verification..

The database 636 or another database (not shown) linked to it may store metadata relating to the video material. Examples of metadata are given in the section M*etadata* below.

The watermark inserter may reinsert the input watermarks in the processed video. However especially if the processor is a mixer the processed video is effectively new material to which a new UMID is associated. Thus the inserter will usually insert a UMID different to the input UMID. The new UMID is preferably stored in the database 636 to link the processed material to its metadata.

UMIDs- Figures 2 and 3.

UMIDs

A UMID is described in reference [2]. Referring to Figure 2, an extended UMID is shown. It comprises a first set of 32 bytes of basic UMID and a second set of 32 bytes of signature metadata.

The first set of 32 bytes is the basic UMID. The components are:

•A 12-byte Universal Label to identify this as a SMPTE UMID. It defines the type of material which the UMID identifies and also defines the methods by which the globally unique Material and locally unique Instance numbers are created.

•A 1-byte length value to define the length of the remaining part of the UMID.

•A 3-byte Instance number which is used to distinguish between different 'instances' of material with the same Material number.

•A 16-byte Material number which is used to identify each clip. Each Material number is the same for related instances of the same material.

The second set of 32 bytes of the signature metadata as a set of packed metadata items used to create an extended UMID. The extended UMID comprises the basic UMID followed immediately by signature metadata which comprises:

•An 8-byte time/date code identifying the time and date of the Content Unit creation.

•A 12-byte value which defines the spatial co-ordinates at the time of Content Unit creation.

•3 groups of 4-byte codes which register the country, organisation and user codes

Each component of the basic and extended UMIDs will now be defined in turn.

The 12-byte Universal Label

The first 12 bytes of the UMID provide identification of the UMID by the registered string value defined in table 1.

Byte No.	Description	Value (hex)
1	Object Identifier	06h
2	Label size	0Ch

3	Designation: ISO	2Bh
4	Designation: SMPTE	34h
5	Registry: Dictionaries	01h
6	Registry: Metadata Dictionaries	01h
7	Standard: Dictionary Number	01h
8	Version number	01h
9	Class: Identification and location	01h
10	Sub-class: Globally Unique Identifiers	01h
11	Type: UMID (Picture, Audio, Data, Group)	01, 02, 03, 04h
12	Type: Number creation method	XXh

Table 1: Specification of the UMID Universal Label

The hex values in table 1 may be changed: the values given are examples. Also the bytes 1-12 may have designations other than those shown by way of example in the table. Referring to the Table 1, in the example shown byte 4 indicates that bytes 5-12 relate to a data format agreed by SMPTE. Byte 5 indicates that bytes 6 to 10 relate to "dictionary" data. Byte 6 indicates that such data is "metadata" defined by bytes 7 to 10. Byte 7 indicates the part of the dictionary containing metadata defined by bytes 9 and 10. Byte 10 indicates the version of the dictionary. Byte 9 indicates the class of data and Byte 10 indicates a particular item in the class.

In the present embodiment bytes 1 to 10 have fixed preassigned values. Byte 11 is variable. Thus referring to Figure 3, and to Table 1 above, it will be noted that the bytes 1 to 10 of the label of the UMID are fixed. Therefore they may be replaced by a 1 byte 'Type' code T representing the bytes 1 to 10. The type code T is followed by a length code L. That is followed by 2 bytes, one of which is byte 11 of Table 1 and the other of which is byte 12 of Table 1, an instance number (3 bytes) and a material number (16 bytes). Optionally the material number may be followed by the signature metadata of the extended UMID and/or other metadata.

The UMID type (byte 11) has 4 separate values to identify each of 4 different data types as follows:

'01h' = UMID for Picture material

'02h' = UMID for Audio material

'03h' = UMID for Data material

'04h' = UMID for Group material (i.e. a combination of related essence).

The last (12th) byte of the 12 byte label identifies the methods by which the material and instance numbers are created. This byte is divided into top and bottom nibbles where the top nibble defines the method of Material number creation and the bottom nibble defines the method of Instance number creation.

Length

The Length is a 1-byte number with the value '13h' for basic UMIDs and '33h' for extended UMIDs.

Instance Number

The Instance number is a unique 3-byte number which is created by one of several means defined by the standard. It provides the link between a particular 'instance' of a clip and externally associated metadata. Without this instance number, all material could be linked to any instance of the material and its associated metadata.

The creation of a new clip requires the creation of a new Material number together with a zero Instance number. Therefore, a non-zero Instance number indicates that the associated clip is not the source material. An Instance number is primarily used to identify associated metadata related to any particular instance of a clip.

Material Number

The 16-byte Material number is a non-zero number created by one of several means identified in the standard. The number is dependent on a 6-byte registered port ID number, time and a random number generator.

Signature Metadata

Any component from the signature metadata may be null-filled where no meaningful value can be entered. Any null-filled component is wholly null-filled to clearly indicate a downstream decoder that the component is not valid.

The Time-Date Format

The date-time format is 8 bytes where the first 4 bytes are a UTC (Universal Time Code) based time component. The time is defined either by an AES3 32-bit audio sample clock or SMPTE 12M depending on the essence type.

The second 4 bytes define the date based on the Modified Julian Data (MJD) as defined in SMPTE 309M. This counts up to 999,999 days after midnight on the 17th November 1858 and allows dates to the year 4597.

The Spatial Co-ordinate Format

The spatial co-ordinate value consists of three components defined as follows:

•Altitude: 8 decimal numbers specifying up to 99,999,999 metres.

•Longitude: 8 decimal numbers specifying East/West 180.00000 degrees (5 decimal places active).

•Latitude: 8 decimal numbers specifying North/South 90.00000 degrees (5 decimal places active).

The Altitude value is expressed as a value in metres from the centre of the earth thus allowing altitudes below the sea level.

It should be noted that although spatial co-ordinates are static for most clips, this is not true for all cases. Material captured from a moving source such as a camera mounted on a vehicle may show changing spatial co-ordinate values.

Country Code

The Country code is an abbreviated 4-byte alpha-numeric string according to the set defined in ISO 3166. Countries which are not registered can obtain a registered alpha-numeric string from the SMPTE Registration Authority.

Organisation Code

The Organisation code is an abbreviated 4-byte alpha-numeric string registered with SMPTE. Organisation codes have meaning only in relation to their registered Country code so that Organisation codes can have the same value in different countries.

User Code

The User code is a 4-byte alpha-numeric string assigned locally by each organisation and is not globally registered. User codes are defined in relation to their registered Organisation and Country codes so that User codes may have the same value in different organisations and countries.

Freelance Operators

Freelance operators may use their country of domicile for the country code and use the Organisation and User codes concatenated to e.g. an 8 byte code which can be registered with SMPTE. These freelance codes may start with the '~' symbol (ISO 8859 character number 7Eh) and followed by a registered 7 digit alphanumeric string.

Metadata- Figure 4

The following is provided, by way of example, to illustrate the possible types of metadata generated during the production of a programme, and one possible organisational approach to structuring that metadata.

Figure 4 illustrates an example structure for organising metadata. A number of tables each comprising a number of fields containing metadata are provided. The tables may be associated with each other by way of common fields within the respective tables, thereby providing a relational structure. Also, the structure may comprise a number of instances of the same table to represent multiple instances of the object that the table may represent. The fields may be formatted in a predetermined manner. The size of the fields may also be predetermined. Example sizes include "Int" which represents 2 bytes, "Long Int" which represents 4 bytes and "Double" which represents 8 bytes. Alternatively, the size of the fields may be defined with reference to the number of characters to be held within the field such as, for example, 8, 10, 16, 32, 128, and 255 characters.

Turning to the structure in more detail, there is provided a Programme Table. The Programme Table comprises a number of fields including Programme ID (PID), Title, Working Title, Genre ID, Synopsis, Aspect Ratio, Director ID and Picturestamp. Associated with the Programme Table is a Genre Table, a Keywords Table, a Script Table, a People Table, a Schedule Table and a plurality of Media Object Tables.

The Genre Table comprises a number of fields including Genre ID, which is associated with the Genre ID field of the Programme Table, and Genre Description.

The Keywords Table comprises a number of fields including Programme ID, which is associated with the Programme ID field of the Programme Table, Keyword ID and Keyword.

The Script Table comprises a number of fields including Script ID, Script Name, Script Type, Document Format, Path, Creation Date, Original Author, Version, Last Modified, Modified By, PID associated with Programme ID and Notes. The People Table comprises a number of fields including Image.

The People Table is associated with a number of Individual Tables and a number of Group Tables. Each Individual Table comprises a number of fields including Image. Each Group Table comprises a number of fields including Image. Each Individual Table is associated with either a Production Staff Table or a Cast Table.

The Production Staff Table comprises a number of fields including Production Staff ID, Surname, Firstname, Contract ID, Agent, Agency ID, E-mail, Address, Phone Number, Role ID, Notes, Allergies, DOB, National Insurance Number and Bank ID and Picture Stamp.

The Cast Table comprises a number of fields including Cast ID, Surname, Firstname, Character Name, Contract ID, Agent, Agency ID, Equity Number, E-mail, Address, Phone Number, DOB and Bank ID and Picture Stamp. Associated with the Production Staff Table and Cast Table are a Bank Details Table and an Agency Table.

The Bank Details Table comprises a number of fields including Bank ID, which is associated with the Bank ID field of the Production Staff Table and the Bank ID field of the Cast Table, Sort Code, Account Number and Account Name.

The Agency Table comprises a number of fields including Agency ID, which is associated with the Agency ID field of the Production Staff Table and the Agency ID field of the Cast Table, Name, Address, Phone Number, Web Site and E-mail and a Picture Stamp. Also associated with the Production Staff Table is a Role Table.

The Role Table comprises a number of fields including Role ID, which is associated with the Role ID field of the Production Staff Table, Function and Notes and a Picture Stamp. Each Group Table is associated with an Organisation Table.

The Organisation Table comprises a number fields including Organisation ID, Name, Type, Address, Contract ID, Contact Name, Contact Phone Number and Web Site and a Picture Stamp.

Each Media Object Table comprises a number of fields including Media Object ID, Name, Description, Picturestamp, PID, Format, schedule ID, script ID and Master ID. Associated with each Media Object Table is the People Table, a Master Table, a Schedule Table, a Storyboard Table, a script table and a number of Shot Tables.

The Master Table comprises a number of fields including Master ID, which is associated with the Master ID field of the Media Object Table, Title, Basic UMID, EDL ID, Tape ID and Duration and a Picture Stamp.

The Schedule Table comprises a number of fields including Schedule ID, Schedule Name, Document Format, Path, Creation Date, Original Author, Start Date, End Date, Version, Last Modified, Modified By and Notes and PID which is associated with the programme ID.

The contract table contains: a contract ID which is associated with the contract ID of the Production staff, cast, and organisation tables; commencement date, rate, job title, expiry date and details.

The Storyboard Table comprises a number of fields including Storyboard ID, which is associated with the Storyboard ID of the shot Table, Description, Author, Path and Media ID.

Each Shot Table comprises a number of fields including Shot ID, PID, Media ID, Title, Location ID, Notes, Picturestamp, script ID, schedule ID, and description. Associated with each Shot Table is the People Table, the Schedule Table, script table, a Location Table and a number of Take Tables.

The Location Table comprises a number of fields including Location ID, which is associated with the Location ID field of the Shot Table, GPS, Address, Description, Name, Cost Per Hour, Directions, Contact Name, Contact Address and Contact Phone Number and a Picture Stamp.

Each Take Table comprises a number of fields including Basic UMID, Take Number, Shot ID, Media ID, Timecode IN, Timecode OUT, Sign Metadata, Tape ID, Camera ID, Head Hours, Videographer, IN Stamp, OUT Stamp. Lens ID, AUTOID ingest ID and Notes. Associated with each Take Table is a Tape Table, a Task Table, a Camera Table, a lens table, an ingest table and a number of Take Annotation Tables.

The Ingest table contains an Ingest ID which is associated with the Ingest Id in the take table and a description.

The Tape Table comprises a number of fields including Tape ID, which is associated with the Tape ID field of the Take Table, PID, Format, Max Duration, First Usage, Max Erasures, Current Erasure, ETA (estimated time of arrival) and Last Erasure Date and a Picture Stamp.

The Task Table comprises a number of fields including Task ID, PID, Media ID, Shot ID, which are associated with the Media ID and Shot ID fields respectively of the Take Table, Title, Task Notes, Distribution List and CC List. Associated with the Task Table is a Planned Shot Table.

The Planned Shot Table comprises a number of fields including Planned Shot ID, PID, Media ID, Shot ID, which are associated with the PID, Media ID and Shot ID respectively of the Task Table, Director, Shot. Title, Location, Notes, Description, Videographer, Due date, Programme title, media title Aspect Ratio and Format.

The Camera Table comprises a number of fields including Camera ID, which is associated with the Camera ID field of the Take Table, Manufacturer, Model, Format, Serial Number, Head Hours, Lens ID, Notes, Contact Name, Contact Address and Contact Phone Number and a Picture Stamp.

The Lens Table comprises a number of fields including Lens ID, which is associated with the Lens ID field of the Take Table, Manufacturer, Model, Serial Number, Contact Name, Contact Address and Contact Phone Number and a Picture Stamp.

Each Take Annotation Table comprises a number of fields including Take Annotation ID, Basic UMID, Timecode, Shutter Speed, Iris, Zoom, Gamma, Shot Marker ID, Filter Wheel, Detail and Gain. Associated with each Take Annotation Table is a Shot Marker Table.

The Shot Marker Table comprises a number of fields including Shot Marker ID, which is associated with the Shot Marker ID of the Take Annotation Table, and Description.

Watermarks-Figures 5 and 6

There is an ever increasing amount of information, and particularly video, being recorded, stored and distributed digitally. The ease with which this information may be duplicated is a concern, since any copyrights in the underlying works may potentially be easily infringed by unauthorised copying. Accordingly, copyright owners may be unwilling to make available and distribute their works without adequate protection against copying, or without being able to demonstrate that a particular example of work originates from them and may be an infringing unauthorised copy.

One possible technique which seeks to provide a solution to this problem is digital watermarking. Digital watermarking allows a code to be embedded in a digital work which contains information which may, for example, identify the owner, the distributor and/or an authorisation code. The digital watermark may be used in conjunction with other deterrents such as encryption.

The digital watermark, hereinafter referred to as the watermark, should be unique such that it, for example, unambiguously identifies the owner, the distributor and/or provides an authorisation code, a technique often referred to a fingerprinting. Also, the watermark may itself be a digital work such as an image, audio or video. The watermark may also contain an indication of whether the work may be copied freely, not copied at all or copied a predetermined number of times.

Preferably, the watermark should be undetectable, unalterable and non-removable by unauthorised individuals. Also, the watermark should not adversely degrade the underlying work in a manner that is readily perceptible. However, the watermark should be readily discernible by authorised individuals such that the owner and/or distributor may be identified.

The watermark should be easily embedded into the underlying digital work. Preferably, the embedding technique should be such that that this can be easily performed during recording, thereby watermarking the work at source, and thus minimising the possibility of any non-watermarked works being available.

The watermark may be placed in, for example, a header or label of a digital work, or the watermark may be embedded within the data fields of the digital work itself. Preferably, the watermark is reproduced many times within a work and, more preferably, is present in every frame of the digital work. Alternatively, the watermark may be placed directly onto the media which carries the digital work.

The watermark may be robust such that it may not be removed or degraded by individuals seeking to make unauthorised copies. Unauthorised attempts to remove the robust watermark should result in severe degradation of the data, rendering the data useless. Situations where the data contains much redundant information, such as in video, may render the robust watermark susceptible to attack by, for example, frame dropping or the like. Hence, the robust watermark should preferably withstand such attacks and may, for example, change from frame to frame and may utilise any error correction/recovery techniques which are applied to data.

Alternatively, the watermark may be fragile such that it is damaged should an unauthorised copy be made.

However, the watermark should also preferably be reversible and removable by the owner, if required. Removal may be particularly useful during, for example, a post-production stage to reduce any cumulative effects of the watermark on the underlying work. Also, where information from different sources are edited together it may be desired that a different watermark is applied to the edited product.

End-user equipment may be configured to recognise the watermark such that it will not allow copying of protected works. Alternatively, the equipment may be configured such that it will only play works originating from a particular owner, distributed through a particular distributor or where the work contains a particular authorisation code.

The watermark may be extracted by comparing watermarked with non-watermarked data and its authenticity established.

Two techniques for embedding a watermark within the data fields of a digital work will now be described in more detail. The first is to embed the watermark in the spatial domain, the second is to embed the watermark in the frequency domain. Both of these embedding processes should be such that they do not result in a significant degradation of the data being watermarked.

Spatial Domain Watermarks

The process, in overview, involves altering predetermined data bits with the bits of a watermark to produce watermarked data. The existence of watermark may be determined by performing the reverse operation on the watermarked data.

One approach is to embed a watermark by substituting insignificant bits of pseudo-randomly selected data with bits representing the watermark. However, these watermarks are susceptible destruction by processing the least significant bits of the data. Another is to insert geometric patterns into the data which represent a watermark. However, these watermarks are susceptible destruction by geometric processing of the data. A further approach is to embed a watermark in a manner which resembles quantisation noise as described with reference to Figure 5 below and more fully described in articles titled "Embedding Secret Information into a Dithered Multi-Level Image" by K Tanaka et al, IEEE Military Communications Conference pages 216-220, 1990 and "Video Steganography" by K Mitsui, IMA Intellectual Property Proceedings, volume 1, pages 187-296, 1994. However, these watermarks are susceptible destruction by signal processing, particularly by requantisation of the data.

Referring now to Figure 5. A source 650 produces a digital data signal 652, such as digital video. A watermark inserter 700 is couple to the source 650 and receives the digital data signal 652. The watermark inserter 700 applies the watermark 663 by applying the watermark to the digital data signal 652 in a manner that resemble requantisation noise to produce watermarked data 705. A storage device 670 is coupled to the watermark inserter 700 and stores the watermarked data 705.

A yet further approach is to randomly select n pairs of image points (a_i, b_i) and increase the brightness of a_i by one while decreasing the brightness of b_i by one. Assuming certain statistical properties of the image are satisfied, the sum of the differences of the n pairs of points will be 2n.

Alternatively, where the data signal comprises at least two components (for example [Y, UV] according to MPEG, PAL or NTC), the watermark may be embedded by assigning values to these components which, in combination, do not usually occur. Also, where a watermark is to be embedded in, for example, video data containing two image fields, a positive watermark may be placed into the first field and a negative watermark into the second field. When watermarked image fields are played there is a masking effect due to the interlacing of the fields and the visual perception of the watermark is significantly reduced.

Frequency Domain Watermarks

The process, in overview, involves obtaining a frequency spectral image of the data to which the watermark is to be applied. The watermark is embedded into predetermined components of the of the frequency spectral image. Thereafter, the watermarked frequency spectral image is subjected to an inverse transform to produce watermarked data. The watermark may be extracted by performing the reverse operation on the watermarked data.

One approach is to partition the data into blocks and compute the Discrete Cosine Transform (DCT) of each of these blocks. Thereafter, the predetermined frequency coefficients of the blocks may be adjusted. A pseudo random subset of blocks may be chosen and in each such block coefficients of predetermined subset of frequencies adjusted such that their relative values encode a data bit. The variance in the relative values and the selection of the predetermined subset of frequencies should be such that the watermark is not perceptible. However, this watermark may be sensitive to damage by noise or further processing.

Alternatively, the watermark may be encoded by adjusting every frequency coefficient by a smaller amount as described with reference to Figure 6 below and more fully described in European Patent Application 0 766 468, NEC Corporation. This has the advantage of making the watermark less sensitive to damage, but increases overall noise levels.

Referring now to Figure 6. A source 650 produces a digital data signal 652, such as digital video. A frequency transformer 655 is coupled to the source 650 and receives the digital data signal 652. The frequency transformer 655 transforms the digital data signal 652 into frequency spectral data 657 using, for example, Discrete Cosine Transforms or Fast Fourier Transform techniques. A watermark inserter 660 is couple to the frequency transformer and receives the frequency spectral data 657. The watermark inserter applies the watermark 663 by adjusting each coefficient of the frequency spectral data 657 to produce watermarked frequency spectral data 663. An inverse frequency transformer 665 is coupled to the watermark inserter 660 and receives the watermarked frequency spectral data 663. The inverse frequency transformer 665 converts the watermarked frequency spectral data 663 into watermarked data 667. A storage device 670 is coupled to the inverse frequency transformer 665 and stores the watermarked data 667.

A further approach is to increase the changes to coefficients in particular frequencies by exploiting the existence of so-called masking phenomena in the human visual and auditory systems. Masking occurs when certain regions of data are occluded by perceptually more prominent regions elsewhere in the data. However, these regions need to be identified prior to inserting the watermark which increases the embedding complexity.

A yet further approach is to compress the digital data and embed the watermark into the x and y co-ordinates of motion vectors of the compressed data. This has the advantage of the watermark being embedded after compression and, hence, is more robust to processing.

Watermark References

Published Articles

- "On the limits of steganography", IEEE Journal on Selected Areas in Communications (J-SAC), Special Issue on Copyright & Privacy Protection, vol. 16 no. 4, pp 474-481, May 1998.
- "Embedding Robust Labels into Images for Copyright Protection", XP 000571967, 1995.
- "Robust Watermarking of Still Images for Copyright Protection", XP 002118119, 1997.
- "Secure Spread Spectrum Watermarking for Images, Audio and Video" IEEE International Conference on Image Processing (ICIP'96), Vol. III, pp. 243-246, 1996.
- "Object-based Transparent Video Watermarking", Electronic Proceedings of the IEEE Signal Processing Society 1997, Workshop on Multimedia Signal Processing, June 1997.
- "Watermarking Methods for MPEG Encoded Video: Towards Resolving Rightful Ownership", Technical Report, University of Illinois at Urbana-Champaign, Number UIUCDCS-R-97-2032, December 1997 (Abstract only).
- "Multimedia Security and Copyright Protection", Technical Report, University of Illinois at Urbana-Champaign, Number UIUCDCS-R-98-2058, September 1998. (Abstract only)

Patent Applications

- EP 0 766 468 "Method and System for Inserting a Spread Spectrum Watermark into Multimedia Data", NEC, 1996.
- WO 96/41468 "Method and Apparatus for Copy Protection for Various Recording Media Using a Video Fingerprint", Macrovision, 1995.
- EP 0 562 787 "Image Coding Method and Apparatus", Canon, 1993.
- US 5,960,081 "Embedding a Digital Signature in a Video Sequence", Cray Research, 1999.
- WO 99/63443 "Methods for Embedding Image, Audio and Video Watermarks in Digital Data", Datamark Technologies, 1998.
- WO 99/22480 "Watermarking of Digital Image Data", Columbia University, 1998.
- WO 99/48290 "Copy Protection Schemes for Copy Protection Digital Material", Philips, 1999.
- WO 99/18723 "Method and Apparatus for a Copy-Once Watermark for Video Recording", Digmarc, 1998.
- WO 98/37513 "Invisible Digital Watermarks", Telstra, 1998.
- WO 97/2206 "Marking a Video and/or Audio Signal", Philips, 1996.
- JP 11-098341 "Electronic Watermark Superimposing Device and Electronic Watermark Detecting Device", Pioneer, 1997.
- US 5,889,868 "Optimisation Methods for the Insertion, Protection, and Detection of Digital Watermarks in the Digitized Data", The Dice Company, 1996.
- US 5,949,885 "Method for Protecting Content Using Watermarking", 1997.
- US 5,664,018 "Watermarking Process Resilient to Collusion Attacks", 1996.

- US 6,021,196 "Reference Palette Embedding", Regents University, 1998.
- US 5,991,426 "Field-based Watermark Insertion and Detection", Signafy, 199
- US 5,905,800 "Method and System for Digital Watermarking", The Dice Company, 1999.
- US 5,809,139 "Watermarking Method and Apparatus for Compressed Digital Video", Vivo Software, 1998.
- US 5,915,027 "Digital Watermarking", NEC, 1999.
- US 6,031,914 "Method and Apparatus for Embedding Data, Including Watermarks, in Human Perceptible Images", University of Minnesota, 2000.
- US 5,745,604 "Identification/Authentication System using Robust, Distributed Coding", Digimarc, 1998.

Modifications

Although for convenience the foregoing describes video processing, the invention may be applied to audio processing. UMIDs are long e.g. 32 or 64 bytes. The material may be identified by an identifier, in the material, and which has fewer bits than a UMID but which links the material to a UMID which uniquely identifies the material.

CLAIMS

1. A video and/or audio material processing system for processing video material including a reversible watermark, the system comprising a remover for removing the watermark, a processor for processing the video material from which the watermark has been removed, and an inserter for inserting a watermark into the processed material.

2. A system according to claim 1, wherein the processor has a user interface for controlling the processes performed thereby.

3. A system according to claim 2, wherein the remover and the inserter are arranged to operate automatically and independently of the user.

4. A system according to claim 1, 2, or 3, further comprising a database processor linked to the remover and to the inserter, the database processor containing data enabling the removal and insertion of the watermark.

5. A system according to claim 4, wherein the said enabling data includes an encryption key.

6. A system according to claim 4 or 5, wherein the inserter and the remover are linked to the database processor by a communications link.

7. A system according to claim 6, wherein the communications link includes the internet.

8. A method of processing video and/or audio material including a reversible watermark, comprising the steps of:
removing the watermark;
processing the material from which the watermark has been removed using a processor; and
inserting a watermark into the processed material.

9. A method according to claim 8, wherein the steps of removing and inserting are automatic and independent of a user of the processor.

10. A method according to claim 9, wherein the removal and insertion are hidden from the user.

11. A method according to claim 8, 9 or 10 further comprising retrieving from a database data enabling the removal and insertion of the watermark.

12. A method according to claim 11, wherein the said enabling data includes an encryption key.

13. A method according to claim 11 or 12, wherein the enabling data is retrieved via communications link.

14. A method according to claim 13, wherein the communications link includes the internet.

15. A processing system substantially as hereinbefore described with reference to the accompanying drawings.

16. A processing method substantially as hereinbefore described with reference to the accompanying drawings.

ABSTRACT

IDENTIFYING MATERIAL

A video processing system processes video material including a reversible watermark. The system comprises a remover for removing the watermark, a processor for processing the video material from which the watermark has been removed, and an inserter for inserting a watermark into the processed material.

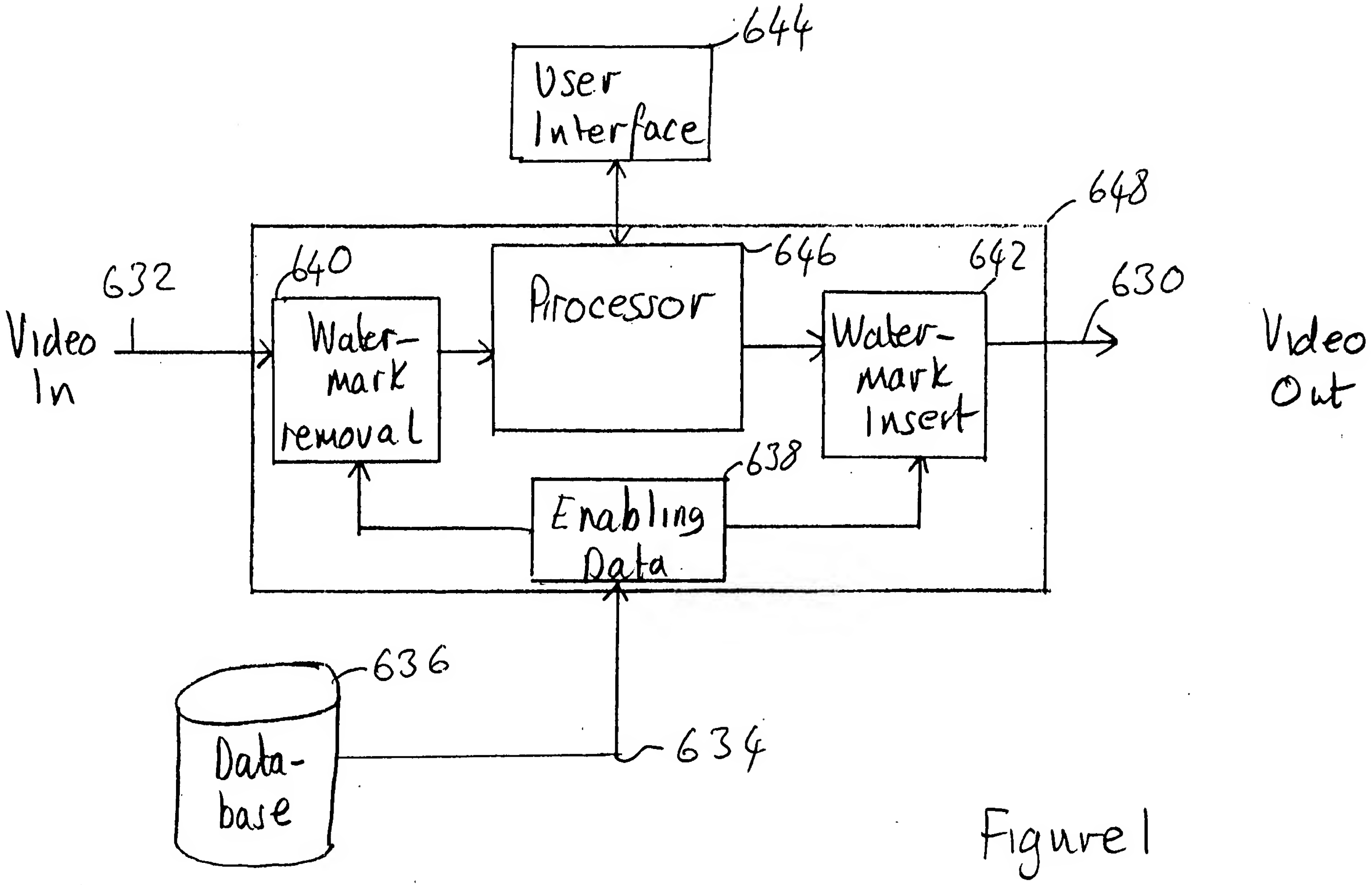
644
User Interface
648
640
646
642
630
632
Video In
Water-mark removal
Processor
Water-mark Insert
Video Out
638
Enabling Data
636
Data-base
634

Figure 1

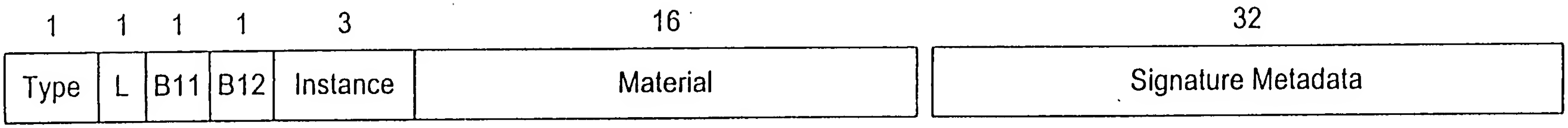

Fig. 3

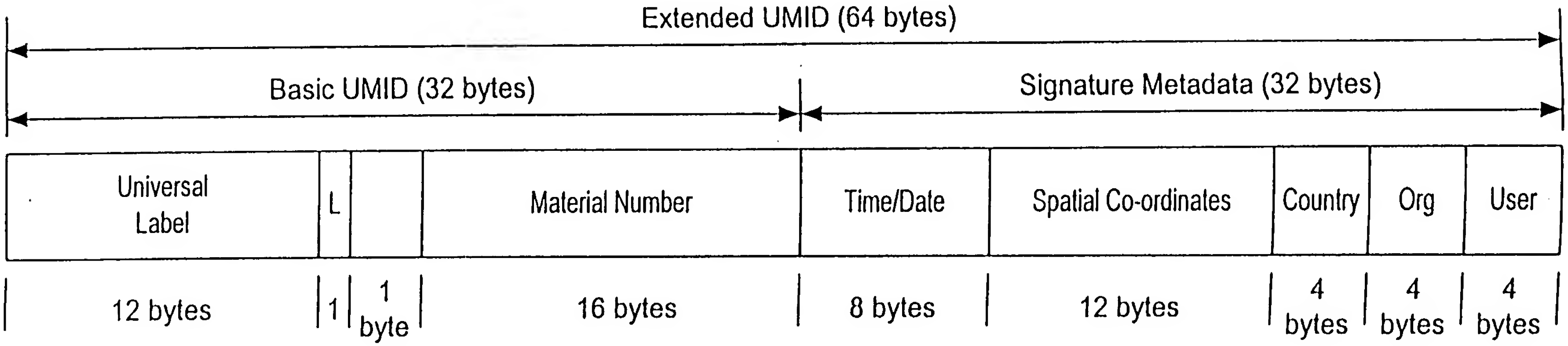

Fig. 2 *Basic and Extended UMID Structures.*

I-00-29

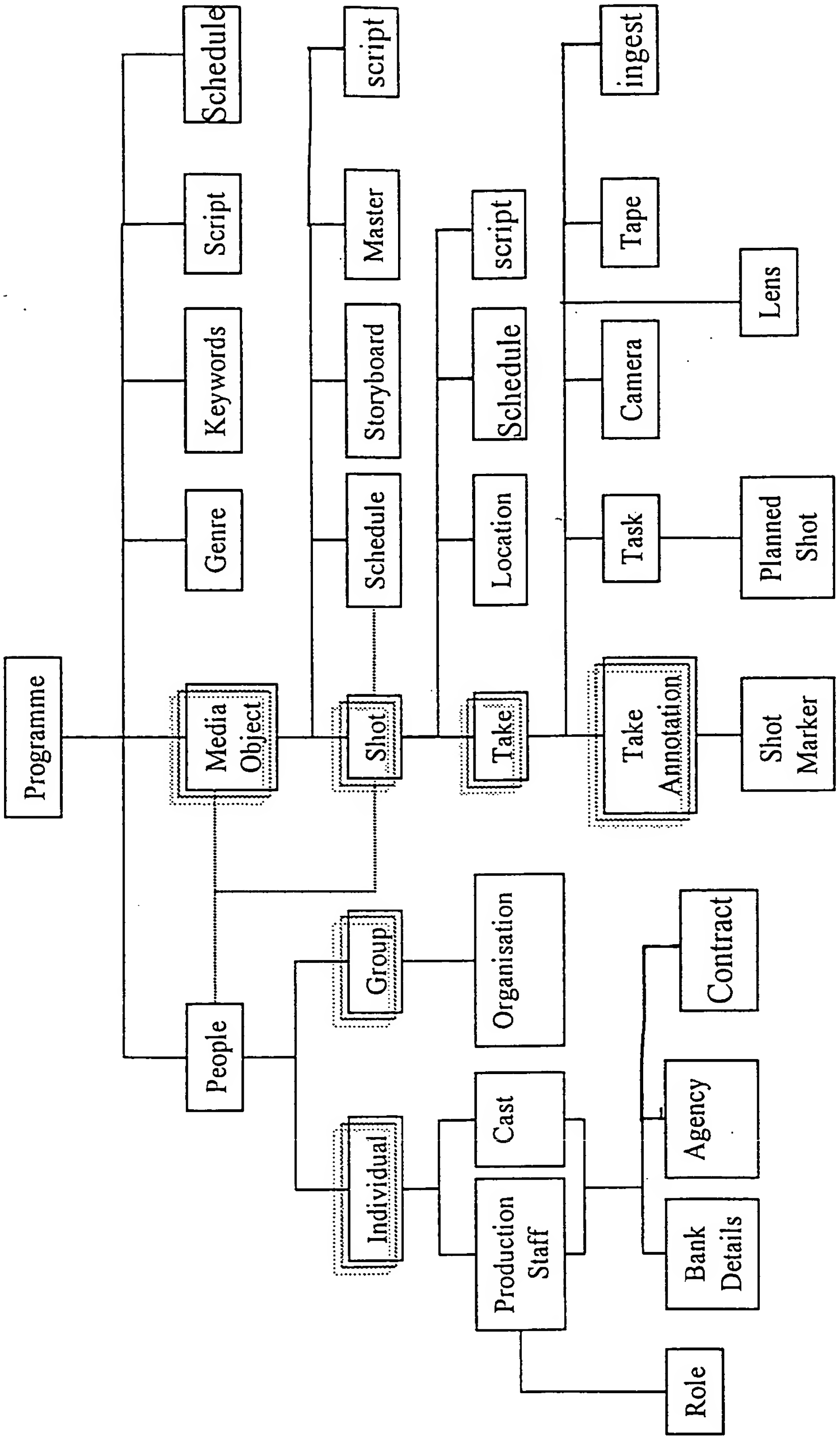
Programme
Genre
Keywords
Script
Schedule
Media Object
Schedule
Storyboard
Master
script
Shot
Location
Schedule
script
Take
Task
Camera
Tape
ingest
Lens
Take Annotation
Planned Shot
Shot Marker
People
Group
Organisation
Individual
Cast
Production Staff
Role
Agency
Bank Details
Contract

Figure 4

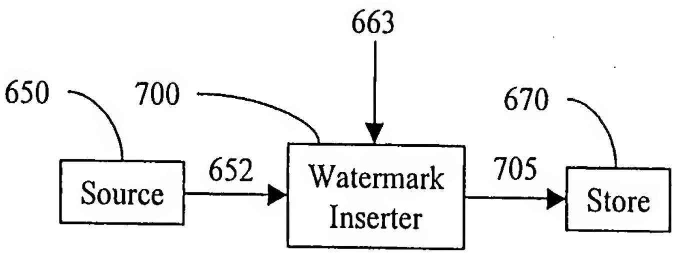

Figure 5

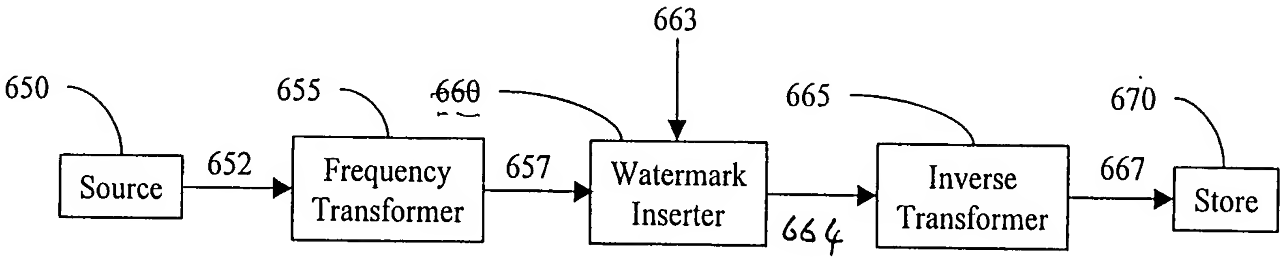

Figure 6